Advisory 2022-05

Security update for CODESYS Control V3 online user management

Published: 06 April 2022

Version: 2.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2022-05_CDS-78845.docx

CONTENT

1 Affected Products

All variants of the following CODESYS V3 products containing the CmpUserMgr component from V3.5.17.0 and before V3.5.18.0 are affected, regardless of the CPU type or operating system:
• CODESYS Control Runtime System Toolkit

Products based on the CODESYS Control Runtime System Toolkit are only affected, if they contain the CmpOPCUAServer component and also register a separate component for anonymous login with the UserMgrRegisterAnonymousLogin() function. These are also concerned, if they register two or more components with the UserMgrRegisterAnonymousLogin() function, in case the CmpOPCUAServer is not included.

In addition, the following products based on the CODESYS Control V3 Runtime System Toolkit are affected in all versions from V4.4.0.0 and before V4.5.0.0:
• CODESYS Control for BeagleBone SL
• CODESYS Control for Beckhoff CX9020 SL
• CODESYS Control for emPC-A/iMX6 SL
• CODESYS Control for IOT2000 SL
• CODESYS Control for Linux SL
• CODESYS Control for PFC100 SL
• CODESYS Control for PFC200 SL
• CODESYS Control for Raspberry Pi SL
• CODESYS Control for WAGO Touch Panels 600 SL

2 Vulnerability overview

2.1 Type

CWE-286: Incorrect User Management [7]

2.2 Management Summary

When the previously enabled anonymous login is deactivated in the security profile settings, it only removes the associated users and groups for one, but not all the registered components. For all others the anonymous access persists.

2.3 References

CVE: CVE-2022-22518 [6]

CODESYS JIRA: CDS-78845

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as medium.

The CVSS v3.1 base score of 6.5 has been assigned. The CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N). [8]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Control runtime system enables embedded or PC-based devices to be a programmable industrial controller. Its central role based user management secures the devices for all online protocols and interfaces. CODESYS Control runtime components can register an anonymous login for their implemented protocols at the user management. This enables the programmer of the controller to allow anonymous access for these protocols and to configure the rights for this access even when the user management is enforced. In the case of OPC UA, for example, he can configure which variables the anonymous user can read or write. In addition, the CODESYS Control runtime security policy can be configured in the communication settings of the CODESYS Development System V3. The policy provides the option of allowing or denying anonymous access for all registered components.

Due to a software flaw, disabling the previously enabled anonymous login in the runtime security policy settings only removes the associated users and groups for one component, but not for all registered components. If more than one component has registered by means of this, anonymous access with the previously configured rights remains permitted for all others.

The CODESYS Control runtime itself registers the CmpOPCUAServer component by default, i.e. as soon as another component is registered, the issue may occur. Specifically, this is the case when a component of an OEM product based on the CODESYS Control Runtime System Toolkit registers for anonymous login using UserMgrRegisterAnonymousLogin(). This interface function is also called by the CODESYS Runtime Extension SL Package of the listed CODESYS Control products and versions, so that these are affected anyway.

3.2 Exploitability

If anonymous logon is deactivated after prior activation, the associated services (e.g. OPC UA) can still be used remotely by anonymous login.

3.3 Difficulty

An attacker with low skills would be able to use the services, if these are still activated unintentionally.

3.4 Existence of exploit

No known public exploits specifically target this vulnerability in CODESYS products.

4 Available software updates

CODESYS GmbH has released version V3.5.18.0, which solves the identified security vulnerability for the following products:
• CODESYS Control Runtime System Toolkit

For the below listed products, the issue will be fixed by version V4.5.0.0, which is based on the CODESYS Control V3 Runtime System Toolkit V3.5.18.10:
• CODESYS Control for BeagleBone SL
• CODESYS Control for Beckhoff CX9020 SL
• CODESYS Control for emPC-A/iMX6 SL
• CODESYS Control for IOT2000 SL
• CODESYS Control for Linux SL
• CODESYS Control for PFC100 SL
• CODESYS Control for PFC200 SL
• CODESYS Control for Raspberry Pi SL
• CODESYS Control for WAGO Touch Panels 600 SL

The release of version V4.5.0.0 is expected for June 2022.

The products available as CODESYS AddOns can be downloaded and installed directly with the CODESYS Installer, which is part of the CODESYS Development System as of version V3.5.17.0.

Alternatively, as well as for all other products, you will find further information on obtaining the software update in the CODESYS Update area [3].

5 Mitigation

CODESYS GmbH recommends using the available software update to fix the vulnerability.

This issue can be worked around by manually removing the corresponding users and groups, in case the software update is not applied:

When allowing anonymous login, users and groups are automatically created for all components registered for anonymous access. After deactivating anonymous login in the runtime security policy settings, these can be manually removed again from the online user management of the device concerned. Using CODESYS

Development System V3, this can be done in the "Users and Groups" device dialog. In case of this bug, after synchronization, users and groups with the prefix "Anonymous_" such as "Anonymous_OPCUAServer" or "Anonymous_PLCShellLinuxBackend" are present. After deleting these users and groups there, anonymous access is no longer possible.

As part of a security strategy, CODESYS GmbH recommends the following general defense measures to reduce the risk of exploits:
• Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside
• Use firewalls to protect and separate the control system network from other networks
• Use VPN (Virtual Private Networks) tunnels if remote access is required
• Activate and apply user management and password features
• Use encrypted communication links
• Limit the access to both development and control system by physical means, operating system features, etc.
• Protect both development and control system by using up to date virus detecting solutions
For more information and general recommendations for protecting machines and plants, see also the CODESYS Security Whitepaper [1].

6 Acknowledgments

The vulnerability was found internally by the CODESYS team.

CODESYS GmbH thanks for reporting following coordinated disclosure. This helps us to improve our products and to protect customers and users.

7 Further Information

For additional information regarding the CODESYS products, especially the above-mentioned versions, or about the described vulnerability please contact the CODESYS support team [5].

8 Disclaimer

Bibliography

[1] CODESYS GmbH: CODESYS Security Whitepaper
[2] CODESYS GmbH: Coordinated Disclosure Policy
[3] CODESYS GmbH update area: https://www.codesys.com/download
[4] CODESYS GmbH security information page: https://www.codesys.com/security
[5] CODESYS GmbH support contact site: https://www.codesys.com/support
[6] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[7] Common Weakness Enumeration (CWE): https://cwe.mitre.org
[8] CVSS Calculator: https://www.first.org/cvss/calculator/3.1
[9] ICS-CERT: https://ics-cert.us-cert.gov

The latest version of this document can be found here:

https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17092&token=a556b1695843bb42084dc63d5bdf553ca02ea393&download=

Change History

Version	Description	Date
1.0	First version	24.03.2022
2.0	Software update available	06.04.2022